

### REMARKS

Claims 1-4, 7-11, 14-23, 28-52 and 56-58 are pending in the action, with claims 1, 8, 15, 20, 28, 33 and 56 being independent.

Claims 1-4, 8-11, 14 and 33-44 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over US Pub. No. 2003/01212791 to **Pickup** in view of USP No. 6,249,805 to **Fleming**, and further in view of US Pub. No. 2003/0023736 to **Abkemeier**.

Claim 7 is rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over **Pickup** and **Fleming** and **Abkemeier**, and further in view of USP No. 6,023,723 to **McCormick**.

Claims 15-19 and 28-32 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over **Pickup** in view of USP No. 7,219,148 to **Rounthwaite**, and further in view of US Pub. No. 2005/0021649 to **Goodman**.

Claims 20-23 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over **Pickup** in view of **McCormick**, and further in view of **Abkemeier**.

Claims 45-49 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over **Pickup** in view of **Fleming** and **Abkemeier**, and further in view of US Pub. No. 2004/0034694 to **Brown**.

Claims 50-52 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over **Pickup** in view of **Fleming** and **Abkemeier**, and further in view of **Rounthwaite**.

Claims 56-58 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over **Pickup** in view of **Fleming**.

Applicant respectfully traverses these rejections. Reconsideration and allowance of the above-referenced application are respectfully requested in light of the following comments and remarks.

#### **Section 103(a) Rejections**

Claims 1-4, 8-11, 14 and 33-44 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over **Pickup** in view of **Fleming**, and further in view of **Abkemeier**. This rejection is respectfully traversed.

Claim 1 recites in part distributing a white list among a plurality of spam filters.

**A. Fleming does not distribute a white list among a plurality of spam filters**

In the statement of rejection, the Examiner asserts that Pickup does not teach or suggest these features, and relies upon col. 5, lines 1-10 of Fleming to cure the deficiencies of Pickup. See page 5, line 17 to page 6, line 5 of the Final Official Action.

Referring to col. 5, lines 1-3, Fleming's electronic mail ("email") system includes an authorization component that maintains a global authorized sender list. An administrator of a company uses the authorization component to ensure that employees do not receive unauthorized email messages. See col. 4, line 65 to col. 5, line 1.

Applicant submits that the relied upon portions of Fleming do not teach or suggest distributing the global authorized sender list among a plurality of spam filters. Fleming's administrator maintains the global authorized sender list, and assigns each email to either a user's inbox or junk mail folder based on whether a sender of the email is on the global authorized sender list. See col. 5, lines 1-3 and lines 14-17. This global authorized sender list is a centralized, system-wide list that is used only by the administrator, not the spam filters associated with the employees. This fact is also recognized by the Examiner in the "Response to Argument" section, in which the Examiner states that "the administrator maintains the global authorized sender list that is shared by all employees." See page 2, item 5, lines 6-7 of the Final Official Action. Since any employee can readily access Fleming's centralized sender list, distributing the global authorized sender list to the employees would be redundant and unnecessary.

Further, as expressly stated at col. 5, lines 8-11, the global authorized sender list serves to relieve each individual employee of maintaining the global authorized sender list, indicating that the global authorized sender list is a centralized list maintained and used only by a single authority -- the administrator. Because the global authorized sender list is controlled and maintained only by a single entity (i.e., Fleming's administrator), Fleming's system need not (and certainly does not) distribute the global authorized sender list to any spam filter (e.g., because doing so would increase manual labor associated with the distribution of the white list and the maintenance of the white list at each spam filter). Indeed, because Fleming's system does not distribute the global authorized sender list, Fleming's system allows an individual

employee to create a personalized sender list local to the employee to suit the employee's needs. See col. 5, lines 11-14. This personalized list, however, also is not distributed to any spam filter associated with any other employee.

**B. Abkemeier does not distribute a white list among a plurality of spam filters**

The Examiner asserts that Abkemeier also discloses the distribution of a white list among a plurality of spam filters at paragraphs [0008] and [0048]. See page 6, lines 16-20 of the Final Official Action.

The relied upon portions of Abkemeier describe an authorization filter (AF) 27 being used as a separate filter for each user that reflects the authorization preferences of an individual user. See [0048]. The AF 27 includes a white list 28 used to determine whether an incoming message is from an authorized or unauthorized sender based on preferences set by the recipient. *Id.*; see also [0050].

Applicant respectfully submits that the relied upon portions of Abkemeier do not teach or suggest distributing a white list among a plurality of spam filters. The relied upon portions of Abkemeier provide an individualized AF 27 having settings that can be modified by an individual user. For example, as stated at paragraph [0035], the AF 27 can utilize filtering algorithms (e.g., a sender-based white list filter algorithm) that an individual message recipient may choose to include to provide message pre-authorization associated with a specific sender. Applicant respectfully submits that the relied upon portions of Abkemeier do not describe the distribution of a white list. Nor do the relied upon portions of Abkemeier provide any teaching or suggestion that the white list 28 used by the AF 27 is distributed among a plurality of spam filters. The relied upon portions of Abkemeier describe the use of a personal sender-based white list. See [0036] and [0039]. Abkemeier's personal sender-based white list is a list defined (e.g., based on sender's email characteristics such as IP address, email address, screen name, etc.) and managed by an individual message recipient. The relied upon portions of Abkemeier do not teach or suggest distributing Abkemeier's personal sender-based white list to a plurality of spam filters. Abkemeier's personal sender-based white list is private and personal to the message recipient, and hence, there is no need to distribute Abkemeier's personal sender-based white list to other spam filters.

Similarly, where the AF 27 is implemented as a single generalized filter for a plurality of users, the relied upon portions of Abkemeier suggest the use of a general shared sender-based white list. *See* [0048]. Abkemeier's general shared sender-based white list filter is established and managed by a party other than the message recipient. *Id.* For example, the general shared sender-based white list filter is provided as a junk mail filter option by email services such as Hotmail, Yahoo, America Online and Earthlink. *See* [0008] and [0013]. Applicant submits that Abkemeier's general shared sender-based white list filter is a centralized white list that is maintained by commercial email service providers. *See* [0040]. The relied upon portions of Abkemeier do not teach or suggest distributing the general shared sender-based white list to any spam filter. Similar to Fleming's global authorized sender list, Abkemeier's general shared sender-based white list filter is controlled and maintained only by a single entity (i.e., Abkemeier's email service provider). The relied upon portions of Abkemeier provide no teaching or suggestion that Abkemeier's email service provider distributes the general shared sender-based white list filter to any spam filter associated with the users.

For at least the foregoing reasons, Applicant respectfully submits that the proposed combination of Pickup, Fleming and Abkemeier does not render claim 1 obvious. Claims 2-4 depend from claim 1, and also are submitted to be allowable for at least the same reasons discussed above with respect to claim 1.

#### **Claim 8**

Claim 8 recites in part determining, using a locally stored list of confirmed senders, if a sender is included in a list of confirmed senders associated with any other spam filter in the network.

In the statement of rejection, the Examiner admits that neither Pickup nor Fleming teach or suggest these features, and relies upon paragraphs [0039], [0048] and [0050] of Abkemeier to cure the deficiencies of Pickup and Fleming. *See* page 9, lines 7-14 of the Final Official Action. Specifically, the Examiner asserts that Abkemeier determines if a sender is included in a list of confirmed senders associated with any other spam filter by using the general shared sender-based white list. *Id.* at lines 14-17.

As a preliminary matter, Abkemeier's general shared sender-based white list is not a

locally stored list of confirmed senders. As discussed above, Abkemeier's general shared sender-based white list filter is established and managed by a party other than the message recipient, and is not locally stored at the recipient. *See* [0040]. Abkemeier's general shared sender-based white list filter is available as a junk mail filter option when users obtain new email accounts, and is maintained by the email service providers while the email accounts remain active. *See* [0008] and [0013].

The relied upon portions of Abkemeier also do not teach or suggest determining if a sender is included in a list of confirmed senders associated with any other spam filter. The relied upon portions of Abkemeier describe that the AF 27 implemented with the general share sender-based white list filter can be used as a single generalized filter or separate filter for each user. *See* [0048]. Where the AF 27 is implemented as a single generalized filter, Applicant respectfully submits that there is no need for Abkemeier to use the AF 27 to determine whether a sender is included in a list of confirmed senders associated with any other spam filter, because Abkemeier's AF 27 would function as a centralized white list for classifying all incoming emails. Where the AF 27 is implemented as a separate filter, Abkemeier's user can set individual filtering preferences that are unique to the user. *See* [0051]. Indeed, the very nature of implementing Abkemeier's AF 27 as a separate filter is to include names of personal contacts whom an individual user has given authorization to send messages. Accordingly, Abkemeier need not use a locally stored white list to determine if a particular sender is included in a list associated with another user, since each individual user white list is tailored to suit each individual user.

For at least the foregoing reasons, Applicant respectfully submits that the proposed combination of Pickup and Fleming does not render claim 8 obvious. Claims 9-11 and 14 depend from claim 8, and also are submitted to be allowable for at least the same reasons discussed above with respect to claim 8.

### Claim 33

Claim 33 recites in part distributing information indicating that a message sender can receive one or more messages among a plurality of spam filters, and using the distributed information at a given one of the plurality of spam filters to determine if a message should be

sent to an intended recipient without separately determining, by a local receiving spam filter, whether the message sender can receive one or more messages.

In the statement of rejection, the Examiner admits that neither Pickup nor Fleming teach or suggest these features, and relies upon paragraphs [0039], [0048] and [0050] of Abkemeier to cure the deficiencies of Pickup and Fleming. See page 12, line 19 to page 13, line 7 of the Final Official Action.

Applicant respectfully submits that the relied upon portions of Abkemeier do not teach or suggest determining if a message should be sent to the recipient without separately determining, by a local receiving spam filter, whether the message sender can receive one or more messages. As discussed at paragraph [0056], the recipient may want to receive a message that is classified as unauthorized. To receive a message from an unauthorized sender, the recipient's email server transmits, to a sender of the unauthorized message, an unauthorized message notification (UMN). See [0057]. If the sender does not respond to the UMN, then the unauthorized message is discarded. See step 48 of FIG. 4. Applicant submits that Abkemeier's sender confirmation process is required regardless of whether the sender has previously been confirmed by another spam filter. As discussed at paragraph [0057], even if the sender may have been a prior (authorized) message sender (e.g., with respect to another recipient), the sender still needs to submit basic identification information in order to acquire proper authorization to send messages to the intended recipient. As such, Abkemeier's system requires that the sender be separately verified by Abkemeier's local filter as to whether the sender can receive messages.

For at least these reasons, Applicant respectfully submits that the proposed combination of Pickup, Fleming and Abkemeier does not render claim 33 obvious. Claims 34-44 depend from claim 33, and also are submitted to be allowable for at least the same reasons discussed above with respect to claim 33.

#### **Section 103(a) Rejections**

Claim 7 is rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over **Pickup** and **Fleming** and **Abkemeier**, and further in view of **McCormick**. The relied upon portions of McCormick do not teach or suggest distributing a white list among a plurality of spam filters, and therefore, also do not cure the noted deficiencies of Pickup, Fleming and Abkemeier.

Claim 7 depends from claim 1, and also is submitted to be allowable for at least the reasons discussed above with respect to claim 1.

### Section 103(a) Rejections

Claims 15-19 and 28-32 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over **Pickup** in view of **Rounthwaite**, and further in view of **Goodman**. This rejection is respectfully traversed.

Claim 15 recites in part collecting information relating to a sender from a plurality of spam filters, determining a trend in the collected information, and identifying a spammer based on the trend.

#### A. Goodman does not collect information from a plurality of spam filters

In the "Response to Argument" section, the Examiner, relying upon paragraph [0011], maintains that Goodman collects information from a plurality of spam filters. *See* page 3, lines 7-9 of the Final Official Action.

Paragraph [0011] refers to assigning a minimum score to an outbound email to determine whether the outbound email is a spam email. For example, a score (e.g., +2) may be assigned to an outbound email when the outbound email contains a URL. *See* [0044]. Another score may be assigned to the outbound email where the score is directly related to the probability of the outbound email being a spam message (e.g., as determined by a machine learning system). *Id.*

The Examiner asserts that the relied upon portions of Goodman describe collecting information relating to a sender from a plurality of spam filters and identifying a trend by determining if the total score associated with an outbound message exceeds a predetermined threshold, and if so, the sender is flagged as a potential spammer. *See* page 3, lines 7-9 of the Final Official Action.

Applicant submits that the scores are assigned based on content extracted from a sender's outbound email, not based on information collected from a plurality of spam filters. The scores are assigned by an administrator of the sender's email service provider as a way to monitor a user's behavior. *See* FIG. 2. There is no indication that Goodman collects any information from a plurality of spam filters. Rather, Goodman extracts information from an outbound email,

where the outbound email is sent to an intended recipient only after the administrator has determined that the outbound email is not a spam email based on the overall score assigned to the outbound email. *See* [0057] – [0060].

**B. Rounthwaite does not determine a trend based on the information collected relating to a sender**

In the “Response to Argument” section, the Examiner maintains that Rounthwaite determines a trend based on information collected relating to a sender because Rounthwaite provides user votes and feedbacks. *See* page 3, lines 7-9 of the Final Official Action.

Applicant submits that Rounthwaite’s user votes and feedbacks are information collected from individual users, not a plurality of spam filters. *See* col. 8, lines 3-10.

Further, the Examiner, citing col. 6, lines 62-66 as support, asserts that Rounthwaite’s machine learning system also can determine a trend based on a “number of messages selected per user or per user per time period, or on the probability of selecting a message from any given user”. *See* page 20, item 37, lines 7-11 of the Final Official Action.

The relied upon portion of Rounthwaite describes a machine learning system for classifying incoming messages as spam messages. *See*, Fig. 1B. Rounthwaite’s machine learning system first receives a series of incoming messages, and identifies the recipients of these messages. *See* col. 5, lines 64-66. Rounthwaite’s machine learning system then selects a subset of the recipients with their respective messages being considered for polling. *See* col. 5, line 66- col. 6, line 7). Polled messages are forwarded to the recipients with voting instructions for voting whether a specific message is a spam. *See* col. 7, lines 19-32. To determine whether to select a message for polling, Rounthwaite’s machine learning system employs the recipients’ demographic information, and other attributes and properties. *See* col. 6, lines 56-60. To prevent a spammer from classifying spam messages as standard messages to skew the overall accuracies of the learning system, Rounthwaite’s machine learning system places restrictions on message selection (e.g., placing limitations on the number of messages that may be polled for a given recipient, or on the probability of selecting a message from any given recipient). *See* col. 6, lines 62-67.



Applicant respectfully submits that the relied upon portion of Rounthwaite pertains to implementing limitations on using or re-using certain messages for training and improving Rounthwaite's machine learning system. As stated in Rounthwaite, without such limitations, a spammer could create an account, send millions of spam messages to the account, and classify all such messages as "good" messages, which would allow the spammer to corrupt Rounthwaite's machine learning system with incorrectly labeled messages. Applicant submits that the relied upon portion of Rounthwaite does not teach or suggest using these limitations to identify a spammer. Rather, the relied upon portion of Rounthwaite describe using the limitations to ensure data integrity of Rounthwaite's machine learning system.

For at least these reasons, Applicant respectfully submits that the proposed combination of Pickup, Goodman and Rounthwaite does not render claim 15 obvious. Claims 16-19 depend from claim 15, and also are submitted to be allowable for at least the same reasons discussed above with respect to claim 15.

#### **Claim 28**

Claim 28 recites in part collecting, using a data center, information relating to a sender from a plurality of the spam filters, and determining a trend in the collected information and identifying the sender as a spammer based on the trend.

However, as discussed above, the relied upon portions of neither Pickup, Rounthwaite nor Goodman teach or suggest these features. For at least these reasons, Applicant respectfully submits that the proposed combination of Pickup, Goodman and Rounthwaite does not render claim 28 obvious.

Claims 29-32 depend from claim 28, and also are submitted to be allowable for at least the same reasons discussed above with respect to claim 28.

#### **Section 103(a) Rejections**

Claims 20-23 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Pickup and McCormick, in view of Abkemeier. This rejection is respectfully traversed.

Claim 20 recites in part if it is determined that a sender is a confirmed message sender, forwarding a received message to a recipient without separately confirming the sender by a spam

filter.

In the statement of rejection, the Examiner admits that neither Pickup nor McCormick teach or suggest these features, and relies upon paragraphs [0039], [0048] and [0050] of Abkemeier to cure the deficiencies of Pickup and McCormick. See page 18, lines 16-22 of the Final Official Action.

However, as discussed above, Abkemeier's system requires that a sender be separately verified by Abkemeier's local filter as to whether the sender can receive messages, even if the sender may have been a prior (authorized) message sender.

For at least these reasons, Applicant respectfully submits that the proposed combination of Pickup, McCormick and Abkemeier does not render claim 20 obvious. Claims 21-23 depend from claim 20, and also are submitted to be allowable for at least the same reasons discussed above with respect to claim 20.

#### **Section 103(a) Rejections**

Claims 45-49 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over **Pickup** in view of **Fleming** and **Abkemeier**, and further in view of **Brown**. The relied upon portions of Brown do not teach or suggest determining if a message should be sent to an intended recipient without separately determining, by a local receiving spam filter, whether the message sender can receive one or more messages, and therefore, also do not cure the noted deficiencies of Pickup, Fleming and Abkemeier.

Claims 45-49 depend from claim 33, and also are submitted to be allowable for at least the same reasons discussed above with respect to claim 33.

#### **Section 103(a) Rejections**

Claims 50-52 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over **Pickup** in view of **Fleming** and **Abkemeier**, and further in view of **Rounthwaite**. The relied upon portions of Rounthwaite do not teach or suggest determining if a message should be sent to an intended recipient without separately determining, by a local receiving spam filter, whether the message sender can receive one or more messages, and therefore, also do not cure the noted deficiencies of Pickup, Fleming and Abkemeier.

Claims 50-52 depend from claim 33, and also are submitted to be allowable for at least the same reasons discussed above with respect to claim 33.

### **Section 103(a) Rejections**

Claims 56-58 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Pickup in view of Fleming.

Claim 56 recites in part distributing a sender's status to other spam filters.

In the statement of rejection, the Examiner admits that Pickup does not teach or suggest these features, but relies on Fleming's personal authorized sender list again to cure the deficiencies of Pickup. See page 24, lines 10-20 of the Final Official Action.

As discussed above, the relied upon portions of Fleming do not teach or suggest distributing status information of a sender to other spam filters. Fleming's personal authorized sender list is retained by a local employee, and is not distributed to anyone in the email network because the sender list is "personalized". Because Fleming's system does not distribute the personal authorized sender list to any other individual, a sender's status (e.g., whether the sender is an authorized sender) is only known to the individual employee who authorizes the sender to send messages. See col. 5, lines 17-19.

For at least these reasons, Applicant respectfully submits that the proposed combination of Pickup and Fleming does not render claim 56 obvious. Claims 57-58 depend from claim 56, and also are submitted to be allowable for at least the same reasons discussed above with respect to claim 56.

### Conclusion

Applicant respectfully requests that all pending claims be allowed.

By responding in the foregoing remarks only to particular positions taken by the Examiner, Applicant does not acquiesce with other positions that have not been explicitly addressed. In addition, Applicant's arguments for the patentability of a claim should not be understood as implying that no other reasons for the patentability of that claim exist.

For all of the reasons set forth above, it is urged that the application is in condition for allowance, an indication of which is respectfully solicited.

If there are any outstanding issues that might be resolved by an interview or an Examiner's amendment, the Examiner is requested to call Applicant's representative at the telephone number shown below.

Please charge any shortage in fees due in connection with the filing of this paper to Deposit Account 06-1050 and please credit any excess fees to such deposit account, referencing Attorney Docket No. 10664-0166001.

Respectfully submitted,

Date: July 9, 2009

/Alex Chan/

Alex Chan

Reg. No. 52,713

Fish & Richardson P.C.  
225 Franklin Street  
Boston, MA 02110  
Telephone: (617) 542-5070  
Facsimile: (877) 769-7945